EMG

Executive Mobility Group B.V

Building The Base A
Evert van de Beekstraat 1-36
1118 CL Schiphol, The Netherlands

WITH YOU ALL THE WAY

+31 (0)20 765 7520
info@executivemobility-group.com
www.executivemobility-group.com

EMG EXECUITIVE MOBILITY SOLUTIONS - CYBER SECURITY MANAGEMENT

At EMG EXECUTIVE MOBILITY SOLUTIONS, we are committed to operating in a socially, environmentally, and economically responsible manner. We recognize the importance of data handling and engaging digitally throughout our company and the world.

We see cyber security as a major threat to business continuity.

We have set a procedure to ensure we mitigate/minimalize the risk for a cyber risk event as well as a procedure what to do if we get hurt by a cyber security incident.

By adopting this corporate sustainability policy, EMG EXECUTIVE MOBILITY GROUP reaffirms its commitment to a sustainable future and invites all employees, clients, and stakeholders to join us in this journey.

Nino Nelissen

CEO

January 2023

EMG

Executive Mobility Group B.V

Building The Base A
Evert van de Beekstraat 1-36
1118 CL Schiphol, The Netherlands

WITH YOU ALL THE WAY

+31 (0)20 765 7520
info@executivemobility-group.com
www.executivemobility-group.com

EMG EXECUITIVE MOBILITY SOLUTIONS - CYBER SECURITY MANAGEMENT

1. Risk Management (see also FD 5.10 Risk Management):

We refer to our Risk Management brochure.

2. Secure configuration:

We have a contract and SLA with an IT company for Managed Services. We refer to this contract as the company provides us with:

- secured configurations on all devices to include:
    - o limited access towards sensitive websites
    - o security warnings for external mails with links
    - o passwords with safe multi-characters and quarterly change
- cloud backup services ▪ virus/ malware scanner update
- allow list of software that may be used, and ensuring continuous safe updates towards the latest versions
    - o Google Chrome as default browser
    - o Microsoft Office 365
    - o Move4U software
    - o Reedge software
- controlled data storage compliant to GDPR

3. Home and mobile working:

In order to allow people to work from home, we do require:

- Only use of authorized equipment (no phone access to data except the CEO)
- Authenticator log-ons
- Confirmed secured internet configurations, duly password protected

4. Incident management:

We refer to our SLA with our Managed IT services. Our incident procedure is defined below. Upon any incident, our IT partner will be called upon immediately for taking the acEons.

EMG

Executive Mobility Group B.V

Building The Base A
Evert van de Beekstraat 1-36
1118 CL Schiphol, The Netherlands

WITH YOU ALL THE WAY

+31 (0)20 765 7520
info@executivemobility-group.com
www.executivemobility-group.com

5. Malware prevention:

Our IT partner ensures optimal malware protection.
During trainings, staff is made aware of the risks and the importance not to click on unknown links and enclosures.
Our IT Partner conducts security tests on a regular base to ensure staff awareness on the risks of opening links etc.

6. Managing user access:

Our CEO indicates the access rights towards the staff, our IT partner ensures the appropriate actions to ensure all staff has the right access rights.

7. Monitoring:

This is part of our SLA with our IT partner, who delivers fully managed services to our company. Any discrepancy or incident is immediately reported to our CEO.

8. Network security:

Staff is aware of risks that come with networks they are connecting their devices to. This subject is part of the training provided on (at least) an annual base and also part of business update meetings.
Our IT partner monitors regular access and based on their automated audits immediately reports certain access or security breaches/risks to Management

9. Removable media controls:

Removable media controls are NOT allowed at any Eme, except for the CEO. The devices are secured for this.

10. Accountability, user education and awareness

Along with our IT partner and our external consultant we have conducted staff trainings that will also be evaluated on an annual base. Also, our IT partner is fully engaged and provides regular security briefings that are shared within the company and our subcontractors.

Our CEO is, along with our carefully selected IT partner, fully responsible for the correct IT infrastructure and the continuously limitation of cyber security risks.